613-001312 Rev.G 121005

最初にお読みください

CentreCOM® AR560S リリースノート

この度は、CentreCOM AR560S をお買いあげいただき、誠にありがとうございました。
このリリースノートは、取扱説明書（613-001301 Rev.A）とコマンドリファレンス（613-001314 Rev.E）の補足や、ご使用の前にご理解いただきたい注意点など、お客様に最新の情報をお知らせするものです。
最初にこのリリースノートをよくお読みになり、本製品を正しくご使用ください。

1　ファームウェアバージョン　2.9.2-09

2　本バージョンで仕様変更された機能

ファームウェアバージョン 2.9.2-07 から 2.9.2-09 へのバージョンアップにおいて、以下の機能が仕様変更されました。

2.1　AS 番号

参照「コマンドリファレンス」/「IP」/「経路制御（BGP-4）」

ADD BGP PEER コマンド /SET BGP PEER コマンドの REMOTEAS パラメーター、SET IP AUTONOMOUS コマンドの AUTONOMOUS パラメーターの指定できる数値の範囲が 1 ～ 65535 に変更されました。

3　本バージョンで修正された項目

ファームウェアバージョン 2.9.2-07 から 2.9.2-09 へのバージョンアップにおいて、以下の項目が修正されました。

3.1　Ethernet インターフェースからパケットが送信される際に、遅延が発生することがありましたが、これを修正しました。

3.2　グローバルアドレスが割り当てられた Android 端末が、NAT 機能を持つ装置配下の AR ルーターに対してリモートアクセス接続を確立できませんでしたが、これを修正しました。

3.3　AR ルーターが Transport モードにて、IPSec 接続を行うイニシエーターとして動作する場合、NAT 機能を持つ装置配下の機器に対して、リモートアクセス接続を確立できませんでしたが、これを修正しました。

4　本バージョンでの制限事項・注意事項

ファームウェアバージョン 2.9.2-09 には、以下の制限事項や注意事項があります。

4.1　認証サーバー

参照「コマンドリファレンス」/「運用・管理」/「認証サーバー」

RADIUS サーバーを複数登録している場合、最初に登録した RADIUS サーバーに対してのみ、SET RADIUS コマンドの RETRANSMITCOUNT パラメーターが正しく動作しません。最初の RADIUS サーバーへの再送回数のみ、RETRANSMITCOUNT の指定値よりも 1 回少なくなります。本現象は 802.1X 認証を使用した場合のみ発生します。

4.2　ログ

参照「コマンドリファレンス」/「運用・管理」/「ログ」

○　複数のログフィルターにそれぞれ複数のログ出力インターフェースを使用する場合、フィルターによって分類されたログメッセージが 1 つのメールで送信されません。

○　スクリプトの実行結果を Syslog サーバーに転送すると、20 行分しか送信されません。

4.3　ETH インターフェース

参照「コマンドリファレンス」/「インターフェース」/「Ethernet インターフェース」

○　RESET ETH COUNTER コマンドを実行しても、ifInOctets カウンターがリセットされません。再度、RESET ETH COUNTER コマンドを実行してください。

○　SHOW ETH COUNTER コマンドで表示される ifOutOctets および ifInOctets の値が送受信したフレームのサイズよりも 8 オクテット多く表示されます。

4.4　ポート認証

参照「コマンドリファレンス」/「運用・管理」/「ポート認証」

○　DISABLE PORTAUTH コマンドで、PORTAUTH パラメーターに 8021X を指定すると、EAP Success パケットを送信してしまいます。

○　RESET ETH コマンドによって Ethernet インターフェースを初期化しても、認証状態は初期化されません。

○　802.1X 認証済みのクライアントがログオフした場合、ログオフしたクライアントの MAC アドレスがフォワーディングデータベース（FDB）に保持されたままになります。

○　ENABLE/SET PORTAUTH PORT コマンドの SERVERTIMEOUT パラメーターが正しく動作しません。これは、SET RADIUS コマンドの TIMEOUT パラメーターと RETRANSMITCOUNT パラメーターの設定が優先されているためです。SET RADIUS コマンドで TIMEOUT × (RETRANSMITCOUNT + 1) の値を SERVERTIMEOUT より大きく設定した場合は、SERVERTIMEOUT の設定が正しく機能します。

4.5　ブリッジング

参照「コマンドリファレンス」/「ブリッジング」

○　ポート 1 がタグ付きパケットのブリッジングの対象となる VLAN に所属し、その VLAN に IP アドレスが設定されている場合、ポート 1 から VLAN の IP アドレス宛ての通信をしようとすると、ルーターが ARP に応答せず、通信ができません。これはポート 1 でのみ発生し、他のポートでは発生しません。

○　SHOW SWITCH COUNTER コマンドで表示される Receive Octets の値が受信したフレームサイズよりも 12 オクテット多く表示されます。

○　SET BRIDGE STRIPVLANTAG コマンドで、ブリッジの際に VLAN タグをはずさない設定にしてある場合、LACP パケットが送信できません。これを回避するには、ETH ポートを使用してください。

4.6　ダイナミック DNS

参照「コマンドリファレンス」/「IP」/「名前解決」

○　ダイナミック DNS のアップデートで、以下の 2 つのケースにおいて、アップデートは再送されません。
- 本製品からの TCP SYN パケットに対して、ダイナミック DNS サーバーからの SYN ACK パケットが返って来ない場合
- 本製品からの TCP SYN パケットに対して、ICMP Host Unreachable メッセージが返される場合

○　ダイナミック DNS のアップデート（HTTP GET）に対する応答として、ダイナミック DNS（HTTP）サーバーから特定のエラーコード（404 Not Found）を受信すると、SHOW DDNS コマンドの Suggested actions の項目に HTML タグの一部が表示されることがあります。

4.7　DNS リレー

参照「コマンドリファレンス」/「IP」/「DNS リレー」

DNS リレー機能有効時、下記条件のとき、クライアントからの名前解決要求に対してクライアントが指定したアドレスとは異なるアドレスで応答します。

○　2 つ以上の VLAN が設定されており、それぞれが異なる IP ネットワークに所属している

○　DNS クライアントが、DNS サーバーのアドレスとして自身が所属していない VLAN の IP アドレスを指定している

これを回避するには、自身が所属している VLAN の IP アドレスを DNS サーバーとして設定してください。

4.8　IPv6

参照「コマンドリファレンス」/「IPv6」

○　RIPng 経路を利用して IPv6 マルチキャスト通信を行っている場合、経路が無効（メトリック値が 16）になっても、しばらくその経路を利用して通信を行います。

○　ガーベージコレクションタイマーが動作中の RIPng 経路は、新しいメトリック値を持つ経路情報を受信しても、タイマーが満了するまで経路情報を更新しません。

4.9　ファイアウォール

参照「コマンドリファレンス」/「ファイアウォール」

○　HTTP プロキシー機能使用時、受信した HTTP パケットに複数の Cookie 要求が含まれている場合、DISABLE FIREWALL POLICY HTTPCOOKIES コマンドを実行していても、その Cookie 要求を破棄せずにフォワードしてしまいます。

○　RTSP、RTP を使用した VoD (Video on Demand) にて RTSP のネゴシエーションよって決定された RTP 受信用の UDP ポート番号を使用した RTP パケットを破棄します。

○　ファイアウォールにてリモート IP を指定せずにダブル NAT ルールを設定すると、ルーターがすべての Gratuitous ARP に対して応答してしまうため、Host にてアドレス重複を検出し、通信できないことがあります。

○　ファイアウォールにて動的に IP アドレスが割り当てられるインターフェースを Public インターフェースとして設定した際、ルール NAT の GBLIP パラメーターに "0.0.0.0" を設定すると、NAT 後のソースアドレスが Public インターフェースの IP ではなく、"0.0.0.0" に変換されるためパケットを送信しません。

○　ファイアウォールにて 3 つ以上のポリシーが設定されているとき、最初のポリシーに設定されているルールが正しく動作しません。

○　ファイアウォール機能有効時、SHOW IP COUNTER コマンドで表示される ETH インターフェースの受信カウンターが実際に受信したパケット数の 2 倍にカウントされます。

○　ファイアウォールルールにマッチするパケットを受信すると SHOW FIREWALL POLICY COUNTER コマンドで表示される Total Packets Received カウンターが実際に受信したパケット数よりも 1 つ多くカウントされます。

○　IPsec とファイアウォール併用時、IPsec 対向機器配下の端末から TELNET でマルチホーミングの設定（追加または削除）を行うと TELNET セッションが削除されます。

○　NAT ループバックの設定で FTP を行うと、3 ウェイハンドシェークが終了しているにもかかわらず、FTP パケットが破棄されます。

4.10　DHCPv6 サーバー

参照「コマンドリファレンス」/「DHCPv6 サーバー」

○　ADD DHCP6 POLICY コマンドで DHCPv6 サーバーの設定を変更しても、サーバーから Reconfigure メッセージが送信されません。ADD DHCP6 POLICY コマンドの実行後、さらに SET DHCP6 POLICY コマンドを実行してください。これにより、Reconfigure メッセージが送信されます。

○　DHCPv6 サーバーで認証機能を使用した場合、ADD DHCP6 KEY コマンドの STRICT パラメーターが動作しません。

4.11 WAN ロードバランス

参照 「コマンドリファレンス」/「WAN ロードバランス」

WAN ロードバランスとファイアウォールの併用時、ポリシーフィルターが適用されている TCP セッションが TCP RST によってクローズすると、該当セッションが WAN ロードバランスセッションに登録されます。

4.12 GRE

参照 「コマンドリファレンス」/「GRE」

GRE 機能有効時、SHOW IP COUNTER コマンドで表示される ETH インターフェースの受信カウンターが実際に受信したパケット数の 2 倍にカウントされます。

4.13 L2TP

参照 「コマンドリファレンス」/「L2TP」

○ ADD L2TP USER コマンドで ACTION パラメーターに dnslookup を指定し、PREFIX パラメーターは未設定とした場合、設定を保存し、再起動するとコンフィグエラーになります。これを回避するには、再起動トリガーで ADD L2TP USER コマンドを再入力してください。

○ L2TP インターフェースで OSPF オンデマンドを使用した場合、L2TP の自動接続を開始しません。

4.14 IPsec

参照 「コマンドリファレンス」/「IPsec」

○ Android OS 標準の VPN クライアントではない独自 VPN クライアントを実装して IPsec DPD に対応したスマートフォン N-06C とリモートアクセス VPN を行うと、N-06C の送信する R-U-THERE メッセージを受信しても本製品は R-U-THEREACK メッセージを返しません。
これを回避するには、PPP LCP エコーの間隔を短くするなどして、通信中は端末側からの IPsec DPD を動作させないようにしてください。

○ SET ISAKMP POLICY コマンドで IPsec DPD と ISAKMP ハートビートを同時に指定すると、DPD の動作モードが正しく反映されません。IPsec DPD と ISAKMP ハートビートを設定する場合には、同時に指定しないようにしてください。

○ SET IPSEC POLICY コマンドを実行した場合、該当する IPsec ポリシー上に確立している IPSec SA が削除されますが、削除された IPSec SA に IP ルートテンプレートが設定されている場合、テンプレートを通じて追加された経路が削除されません。
DELETE IP ROUTE コマンドで該当する IP ルート情報を削除することにより、この不整合から復旧させることができます。

5　取扱説明書とコマンドリファレンスについて

最新の取扱説明書（613-001301 Rev.A）とコマンドリファレンス（613-001314 Rev.E）は弊社ホームページに掲載されています。
本リリースノートは、上記の取扱説明書とコマンドリファレンスに対応した内容になっていますので、お手持ちの取扱説明書、コマンドリファレンスが上記のものでない場合は、弊社 Web ページで最新の情報をご覧ください。

※パーツナンバー「613-001314 Rev.E」は、コマンドリファレンスの全ページ（左下）に入っています。

http://www.allied-telesis.co.jp/